UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

T.S., individually and on behalf of all others similarly situated, *Plaintiff*, *v.* BODY CONTOUR CENTERS, LLC d/b/a SONO BELLO, a Delaware limited liability company, *Defendant*.	Case No. CLASS ACTION COMPLAINT JURY DEMAND

Plaintiff T.S. ("Plaintiff") brings this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Defendant Body Contour Centers, LLC d/b/a Sono Bello ("Defendant" or "Sono Bello"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. Defendant Body Contours Centers, LLC owns and operates a national network of medical facilities under the brand name Sono Bello. Sono Bello advertises itself as "America's

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

#1 Cosmetic Surgery Specialist"[1] with "150+ board-certified surgeons."[2]

2. Sono Bello clinics offers various medical weight loss treatments, including laser liposuction, micro-laser liposuction, cellulite reduction procedures, and excess skin removal surgeries. All of Defendant's services are performed by trained medical professionals.

3. Sono Bello operates a website, https://sonobello.com/ (the "Website"), which allows for the online booking of medical appointments.

4. When booking medical services online, patient privacy is crucial. Patients expect, as they should, that their information will be held in confidence and not shared with third parties without their knowledge or consent. The sensitive nature of information related to weight loss and body image amplifies the need for privacy during online bookings. Weight loss procedures often involve deeply personal details about an individual's physical appearance, struggles with body image, and health history. This information can be emotionally charged and stigmatizing, making the protection of such data especially critical.

5. Moreover, information concerning an individual's healthcare, including medical procedures, is protected by state and federal law. Despite these protections and Defendant's duty as a healthcare provider, Defendant aided, employed, agreed, and conspired with Facebook[3] to intercept sensitive and confidential communications sent and received by Plaintiff and Class Members, including communications containing protected medical information.

6. This is a class action lawsuit brought on behalf of all California residents who have accessed and used the Website to book a consultation with Defendant.

---

[1] https://pages.sonobello.com/brand-ff-2024/?camp_id=9063&utm_term=sono%20bello&utm_campaign=Search+-+Branded++Miami&utm_source=adwords&utm_medium=ppc&hsa_acc=6103458045&hsa_cam=20737047585&hsa_grp=154892348123&hsa_ad=711709476195&hsa_src=g&hsa_tgt=kwd11804729825&hsa_kw=sono%20bello&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQiA6Ou5BhCrARIsAPoTxrA_eOqmxEQKJ9ibLKmDtN-zJ9uCoODQeQip2bwwNjo6N1IGPEGlk5kaAp3lEALw_wcB

[2] https://www.sonobello.com/

[3] In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced collectively as "Facebook."

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

7. Plaintiff seeks an order (i) declaring that Defendant's conduct violates the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1); (ii) violates the California Invasion of Privacy Act, Cal. Penal Code § 631; (iii) violates the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10; (iv) requiring Defendant to cease the unlawful activities discussed herein; and (v) awarding statutory damages to Plaintiff and the proposed Classes (defined below).

PARTIES

8. Plaintiff T.S. is an adult citizen of the state of California and is domiciled in Sunnyvale, California. Plaintiff has actively maintained her Facebook account at all relevant times prior to and after booking a consultation through the Website.

9. In or around October 2023, Plaintiff used the Website to book a consultation for a surgical weight loss procedure. Pursuant to the systematic process described herein, Defendant assisted Facebook with intercepting Plaintiff's communications, including those that contained Personally Identifiable Information ("PII"), Protected Health Information ("PHI"), and related confidential information, as described more thoroughly below. Defendant assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. As a consequence of these interceptions, Plaintiff has received targeted advertisements from Facebook marketing for weight loss procedures. Due to the surreptitious nature of the interceptions at issue, Plaintiff was not aware that Defendant assisted Facebook in unlawfully intercepting her PII and PHI until approximately May 2024.

10. Defendant Body Contours Centers, LLC owns and operates a national network of medical facilities that offers various cosmetic surgeries and procedures. Defendant is incorporated in Washington with its principal place of business at 5250 Carillon Point, Kirkland, WA 98033.

11. Defendant owns and operates the Website, https://sonobello.com/, whereby consumers seeking to procure medical treatment can schedule in-person consultations for its medical services. This includes its patented Trisculpt liposuction technique, as well as laser

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

liposuction, micro-laser liposuction, cellulite reduction procedures, and excess skin removal surgeries. Its Website offers consumers access to its services through online booking of in-person consultations with medically trained surgeons.

12. At all relevant times, Defendant's Website hosted code for the Facebook Tracking Pixel, as described more thoroughly below.

13. By failing to receive the requisite consent, Defendant breached its duties of confidentiality and unlawfully disclosed Plaintiff's PII and PHI.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court also has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from at least one defendant.

15. The Court has personal jurisdiction over Defendant because Defendant is licensed to conduct business in this District and maintains its headquarters and principal place of business in this District.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant is licensed to conduct business in this District and its headquarters and principal place of business are maintained in this District.

FACTUAL ALLEGATIONS

I. Background of the California Information Privacy Act.

17. The California Information Privacy Act ("CIPA"), California Penal Code section 630, *et seq.*, prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

sent from or received at any place within California.

18. To establish liability under California Penal Code section 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

19. Section 631(a)'s applicability is not limited to phone lines, but also applies to "new technologies" including computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

II. Warning on Tracking Codes on Health Care Websites.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

20. The federal government has issued guidance warning that tracking code, like the Facebook Tracking Pixel, may violate federal privacy law when installed on healthcare websites such as Defendant's. The statement titled, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (the "Bulletin"), was issued by the Department of Health and Human Services' Office for Civil Rights ("OCR") in December 2022.[4]

21. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act ("HIPAA") may use third-party tracking tools, such as the Facebook Tracking Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures***.[5]

22. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI***. Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment***. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more***

[4] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (Mar. 18, 2024).

[5] *Id.* (Emphasis added).

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

> ***than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[6]

23. Plaintiff and Class Members face the risks about which the government expresses concern. Defendant disclosed the fact that Plaintiff's and Class Members' booked body contouring medical procedures on Defendant's Website, which in turn also discloses the health conditions for which they seek a health care provider; the frequency with which they take steps relating to body image; and where they seek medical treatment. This information is, as described by the OCR in its bulletin, "highly sensitive."

24. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.[7]

25. Crucially, that paragraph in the government's Bulletin continues:

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care***.[8]

26. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use

[6] *Id.* (Emphasis added).

[7] *Id*. (Emphasis added).

[8] *Id*. (Emphasis added).

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.

"When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

"Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."

The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.

In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.

. . . Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC's Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule . . . .[9]

[9] FEDERAL TRADE COMMISSION, FTC AND HHS WARN HOSPITAL SYSTEMS AND TELEHEALTH PROVIDERS ABOUT PRIVACY AND SECURITY RISKS FROM ONLINE TRACKING TECHNOLOGIES, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

27. Therefore, Defendant's conduct is directly contrary to clear pronouncements by the FTC and HHS.

28. In light of, and in addition to, the federal government's own issued guidance above, news sources also warn that tracking code, like the Facebook Tracking Pixel, poses risks of violating federal privacy law and HIPAA: Federal regulators are warning [regulated entities] hospital systems and telehealth providers about the data privacy risks of using third-party tracking technologies.

> These services, like [Facebook Tracking] Pixel or Google Analytics, could violate the Health Insurance Portability and Accountability Act (HIPAA) or Federal Trade Commission (FTC) data security rules, officials said.
>
> The FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a rare joint release announcing that 130 [regulated entities] hospital systems and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps … "The compliance buck still stops with you. Furthermore, your company is legally responsible even if you don't use the data obtained through tracking technologies for marketing purposes."[10]

29. Fierce Healthcare also spoke up in an April 3, 2023 article:

> Nearly all nonfederal acute care hospitals' [regulated entities'] websites track and transfer data to a third party, potentially fueling the unwanted disclosures of patients' sensitive health information and opening up that [regulated entity] hospital to legal liability, according to a recently published University of Pennsylvania analysis. [https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2022.01205]. The census of more than 3,700 hospital [regulated entity] homepages found at least one third-party data transfer among 98.6% of the websites as well as at least one third-party cookie on 94.3%, researchers wrote in Health Affairs.

30. Health Affairs also published an article in April 2023, stating:

> The hospitals' [regulated entities'] homepages had a median of 16 third-party transfers, more of which were found among medium-sized (100 to 499 beds) hospitals, nonprofit hospitals, urban hospitals, health system-affiliated hospitals and those that weren't serving the largest portion of patients in poverty, they wrote … Many of these complaints cite Facebook parent company Meta's Pixel tracker,

[10] Heather Landi, *Regulators warn hospitals and telehealth companies about privacy risks of Meta, Google tracking tech*, FIERCE HEALTHCARE, July 21, 2023, https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

> which a June 2022 investigation from The Markup [https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites] detected on about a third of large hospitals' websites. That report found evidence that, in some instances, the sensitive data transferred to third parties met the criteria for a HIPAA violation.[11]
>
> By including third-party tracking code on their websites, hospitals [regulated entities] are facilitating the profiling of their patients by third parties. These practices can lead to dignitary harms, which occur when third parties gain access to sensitive health information that a person would not wish to share. These practices may also lead to increased health-related advertising that targets patients, as well as to legal liability for hospitals [regulated entities].[12]

31. This is further evidence that the data that Defendant chose to share is protected PII and PHI. The sharing of that information was a violation of Class Members' rights.

III. Facebook's Platform and its Business Tools.

32. Facebook describes itself as a "real identity platform,"[13] meaning users are allowed only one account and must share "the name they go by in everyday life."[14] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[15]

---

[11] Dave Muoio, *Almost every hospital's homepage is sending visitors' data to third parties, study finds*, FIERCE HEALTHCARE, Apr. 3, 2023, https://www.fiercehealthcare.com/providers/almost-every-hospital-homepage-sending-visitors-data-third-parties-study-finds.

[12] Ari B. Friedman, et al., *Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals*, HEALTH AFFAIRS, Vol. 42, No. 24, Apr. 2023, https://www.healthaffairs.org/doi/10.1377/hlthaff.2022.01205.

[13] Sam Schechner & Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[14] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

[15] FACEBOOK, SIGN UP, https://www.facebook.com.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

33. In 2023, Facebook generated over $134 billion in revenue.[16] With respect to the apps offered by Facebook, substantially all of Facebook's revenue is generated by selling advertising space.[17]

34. Facebook sells advertising space by highlighting its ability to target users.[18] Facebook can target users so effectively because it surveils user activity both on and off its website.[19] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[20] Facebook compiles this information into a generalized dataset called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[21]

35. Advertisers can also build "Custom Audiences."[22] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[23] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverage[] information such as demographics, interests, and behavior from

---

[16] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS; INITIATES QUARTERLY DIVIDEND 1, 1 (Feb. 1, 2024), https://s21.q4cdn.com/399680738/files/doc_financials/2023/q4/Meta-12-31-2023-Exhibit-99-1-FINAL.pdf.

[17] *Id.* at 10.

[18] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

[19] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[20] FACEBOOK, AUDIENCE AD TARGETING: HOW TO FIND PEOPLE MOST LIKELY TO RESPOND TO YOUR AD, https://www.facebook.com/business/ads/ad-targeting.

[21] FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[22] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[23] FACEBOOK, AUDIENCE AD TARGETING: HOW TO FIND PEOPLE MOST LIKELY TO RESPOND TO YOUR AD, https://www.facebook.com/business/ads/ad-targeting.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

your source audience to find new people who share similar qualities."[24] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers or by utilizing Facebook's "Business Tools."[25]

36. As Facebook puts it, the Business Tools "help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[26] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

37. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[27] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from

---

[24] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[25] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

[26] FACEBOOK, THE META BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

[27] *See* FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

which advertisers can choose, including what content a visitor views or purchases.[28] Advertisers can even create their own tracking parameters by building a "custom event."[29]

38. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their website. As the name implies, the Facebook Tracking Pixel "tracks the people and type of actions they take."[30] When a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to contemporaneously send a separate message to Facebook's servers. This second secret and contemporaneous transmission contains the original GET request sent to the host website, along with additional data that the Facebook Tracking Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. At relevant times, two sets of code were thus automatically run as part of the browser's attempt to load and read https://sonobello.com—Defendant's own code and Facebook's embedded code.

39. An example illustrates the point. Take an individual who, at relevant times, navigated to https://sonobello.com/ and, as Plaintiff did, requested a consultation by clicking the "Schedule Free Consultation" or "Book Online" icons. When clicked, the individual's browser sent a GET request to Defendant's server requesting that server to load the particular webpage. As a result of Defendant's use of the Facebook Tracking Pixel, Facebook's embedded code, written in JavaScript, sent secret instructions back to the individual's browser, without alerting the individual that this was happening. Facebook caused the browser to secretly duplicate the communication with Defendant, transmitting it to Facebook's servers, alongside additional

---

[28] FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

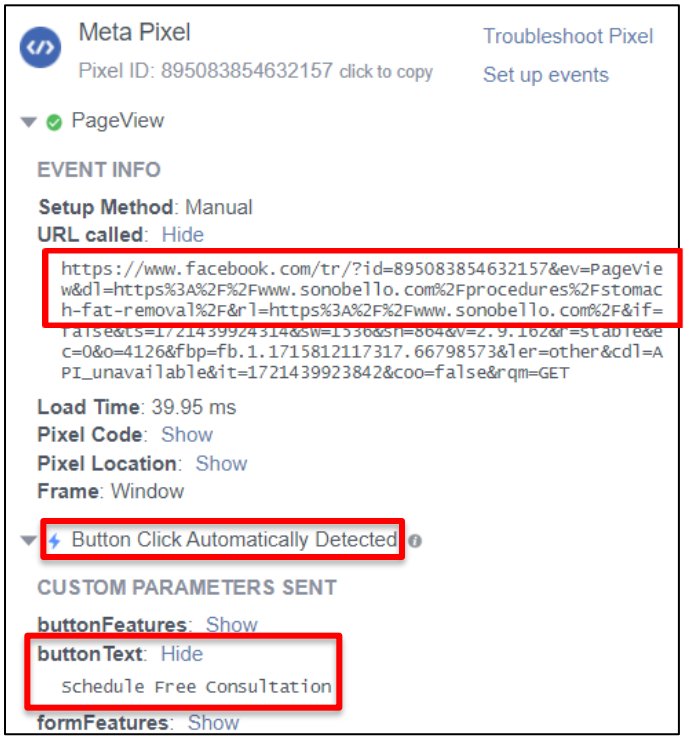
[29] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[30] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

information that transcribed the communication's content and the individual's identity. *See* Figure 1.

Figure 1:



40. As seen in Figure 1, through the Facebook Tracking Pixel, Defendant assists Facebook in receiving confidential information from consumers seeking to procure medical services, including their Facebook ID.

41. After collecting and intercepting the information described in the preceding paragraph, Facebook processed it, analyzed it, and assimilated it into datasets like Core Audiences and Custom Audiences for targeted advertising purposes.

IV. How Defendant Disclosed Plaintiff's and Class Members' PII and PHI and Assisted With Intercepting Communications.

42. Through the Facebook Tracking Pixel, Defendant shared its patients' online activity, including their sensitive and confidential information and search results, including information related to the weight loss surgical procedures it provides.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

43. For example, as alleged above, when a patient entered the Website and requested a consultation, Defendant transmitted information relating to the specific patient's consultation to Facebook via the Facebook Tracking Pixel.

44. Each time Defendant sent this activity data, it also disclosed patients' PII, including their Facebook ID. A Facebook ID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique Facebook ID, so too can any ordinary person who comes into possession of a Facebook ID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the Facebook ID can connect to any Facebook profile.

45. A user who accessed https://sonobello.com/ while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

46. When a visitor's browser had recently logged out of an account, Facebook compelled the visitor's browser to send a smaller set of cookies.

47. One such cookie was the "fr cookie" which contained, at least, an encrypted Facebook ID and browser identifier. [31] Facebook, at a minimum, used the fr cookie to identify users. [32]

48. If a visitor had never created an account, an even smaller set of cookies was transmitted.

49. At each stage, Defendant also utilized the "_fbp cookie," which attached to a browser as a first-party cookie, and which Facebook used to identify a browser and a user. [33]

---

[31] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT 1, 33-34 (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

[32] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[33] *Id.*

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

50. The c_user cookie expires after 90 days if the user checked the "keep me logged in" checkbox on the website.[34] Otherwise, the c_user cookie is cleared when the browser exits.[35]

51. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[36] If that happens, the time resets, and another 90 days begins to accrue.[37]

52. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[38] If that happens, the time resets, and another 90 days begins to accrue.[39]

53. The Facebook Tracking Pixel used both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, https://sonobello.com/.[40] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*, www.facebook.com.[41] The _fbp cookie was always transmitted as a first-party cookie. A duplicate _fbp cookie was sometimes sent as a third-party cookie, depending on whether the browser had recently logged into Facebook.

54. Facebook, at a minimum, used the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles. Defendant sent these identifiers alongside the event data.

---

[34] Seralahthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019), https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a.

[35] *Id.*

[36] *See id.*

[37] Confirmable through developer tools.

[38] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[39] Also confirmable through developer tools.

[40] PC MAG, FIRST-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[41] PC MAG, THIRD-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable by tracking network activity.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

V. Plaintiff Never Provided Defendant or Facebook with Consent to Intercept Her Sensitive and Confidential PHI or PII.

55. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose her confidential and sensitive PII. Plaintiff was never provided with any written notice that Defendant disclosed the users of the Website nor was she provided with any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed to Facebook her sensitive and confidential PII.

56. Facebook likewise never received consent to intercept sensitive, protected information. In fact, Facebook expressly warrants the opposite, promising to shield that information from disclosure.

57. When first signing up, a Facebook user assents to three agreements: the Terms of Service,[42] the Cookies Policy,[43] and the Data Policy.[44]

58. Facebook's Terms of Service begins by stating that "[p]rotecting people's privacy is central to how we've designed our ad system."[45] The Terms of Service then prohibits anyone from using Facebook's Products in a manner that is "unlawful, misleading, discriminatory or fraudulent."[46]

59. Facebook's Data Policy recognizes that there may be "[d]ata with special protections," meaning information that "could be subject to special protections under the laws of your country."[47] The Data Policy goes on to describe how Facebook collects information from its "Meta Business Tools," including "our social plug-ins (such as the Like button), Facebook

---

[42] FACEBOOK, TERMS OF SERVICE, https://www.facebook.com/legal/terms/update.

[43] FACEBOOK, COOKIES POLICY, https://www.facebook.com/policies/cookies/.

[44] FACEBOOK, DATA POLICY, https://m.facebook.com/about/privacy/update/printable.

[45] FACEBOOK, TERMS OF SERVICE, https://www.facebook.com/legal/terms/update.

[46] *Id.*

[47] FACEBOOK, DATA POLICY, https://m.facebook.com/about/privacy/update/printable.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

Login, our APIs and SDKs, or the Meta pixel."[48] Specifically, Facebook acknowledges that "[p]artners receive your data when you visit or use their services or through third parties they work with."[49]

60. Facebook then offers an express representation: "**We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us**."[50] Facebook does acknowledge collecting "data with special protections" to personalize ads, but critically, only sensitive information that users "choose to provide."[51]

61. Facebook's Cookies Policy ratifies those representations, stating "the Data Policy will apply to our processing of the data that we collect via cookies."[52]

62. Facebook's other representations further reinforce these warranties. In its Advertising Policy, Facebook states "[w]e do not use sensitive personal data for ad targeting."[53] And in a blog post titled "About Restricted Meta Business Tools Data," Facebook asserts it has "policies around the kinds of information businesses can share with us."[54] Facebook does not "want websites or apps sending us sensitive information about people."[55] Sensitive information includes, among other things, "any information defined as sensitive under applicable laws, regulations and applicable industry guidelines."[56]

---

[48] *Id.*

[49] *Id.*

[50] *Id.* (Emphasis added).

[51] *Id.*

[52] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policies/cookies/.

[53] FACEBOOK, INTRODUCTION TO ADVERTISING STANDARDS, https://www.facebook.com/policies/ads/.

[54] FACEBOOK, ABOUT RESTRICTED META BUSINESS TOOLS DATA, https://www.facebook.com/business/help/1057016521436966?id=188852726110565.

[55] *Id.*

[56] *Id.*

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

63. These representations are repeated frequently. Facebook created a "Help Center" to better explain its practices to users. In an article titled, "How does Facebook receive information from other businesses and organizations?," Facebook reiterates its promise to "prohibit businesses or organizations from sharing sensitive information with us," and if Facebook "determine[s] that a business or an organization is violating our terms, we'll take action against that business or organization."[57] In another article, titled, "How does Meta work with data providers?," Facebook repeats this promise, stating "[b]usinesses that advertise on Facebook are required to have any necessary rights and permissions to use this information, as outlined in our Custom Audience Terms that businesses must agree to."[58]

64. Based on these representations, Facebook never receives consent from users to intentionally intercept and monetize electronic communications disclosing sensitive information that the law protects.

CLASS ALLEGATIONS

65. **Class Definition**: Plaintiff brings this on behalf of herself and a class defined as all persons in the United States who, during the class period, maintained a Facebook account and accessed https://sonobello.com to book a consultation (the "Class").

66. Plaintiff also seeks to represent a subclass defined as all persons in California who, during the class period, maintained a Facebook account and accessed https://sonobello.com to book a consultation (the "California Subclass").

67. The following people are excluded from the Classes: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former employees, officers and directors; (3)

[57] FACEBOOK, HOW META RECEIVES INFORMATION FROM OTHER BUSINESSES AND ORGANIZATIONS, https://www.facebook.com/help/2230503797265156.

[58] HOW DOES META WORK WITH DATA PROVIDERS?, https://www.facebook.com/help/494750870625830?ref=dp.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

68. **Numerosity**: On information and belief, tens of thousands of consumers fall into the definition of the Classes. Members of the Classes can be identified through Defendant's records, discovery, and other third-party sources.

69. **Commonality and Predominance**: There are many questions of law and fact common to Plaintiff's and the Classes claims, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. whether Defendant intentionally assisted a third party with tapping the lines of internet communication between itself and customers;

b. Whether Defendant's Website surreptitiously recorded PII, PHI, and related communications itself and its customers;

c. Whether Facebook was a third-party eavesdropper;

d. Whether Defendant's disclosures of PII, PHI, and related communications constituted an affirmative act of communication;

e. Whether Defendant's conduct, which allowed Facebook—an unauthorized person—to view Plaintiff's and Class Members' PII and PHI, resulted in a breach of confidentiality;

f. Whether Defendant violated Plaintiff's and Class Members' privacy rights by using the Facebook Tracking Pixel to record and communicate their Facebook IDs alongside their confidential medical communications; and

g. Whether Plaintiff and Class Members are entitled to damages under the ECPA, CIPA, CMIA, or any other relevant statute.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

70. **Typicality**: Plaintiff's claims are typical of the claims of other members of the Classes in that Plaintiff and the members of the Classes sustained damages arising out of Defendant's wrongful conduct.

71. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the other members of the Classes.

72. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Classes and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's actions that Plaintiff challenges apply and affect members of the Classes uniformly, and Plaintiff's challenge of these actions hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff. The factual and legal bases of Defendant's liability to Plaintiff and to the other members of the Classes are the same.

73. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. The harm suffered by the individual members of the Classes is likely to have been relatively small compared to the burden and expense of prosecuting individual actions to redress Defendant's wrongful conduct. Absent a class action, it would be difficult if not impossible for the individual members of the Classes to obtain effective relief from Defendant. Even if members of the Classes themselves could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

to all parties and the Court and require duplicative consideration of the legal and factual issues presented. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

74. Plaintiff reserves the right to revise the "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act,
18 U.S.C. § 2511(1)
(On behalf of Plaintiff and the Class)

75. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

76. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

77. The ECPA protects both sending and the receipt of communications.

78. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

79. The transmission of Plaintiff's private and confidential information to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

80. The transmission of the private and confidential information between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

of 18 U.S.C. § 2510(12).

81. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

82. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

83. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

84. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Facebook used to track Plaintiff and Class Members communications while they were navigating the Website;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' mobile devices;

d. Defendant and Facebook's web and ad servers;

e. The plan Defendant and Facebook carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

85. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

86. By utilizing and embedding the Facebook Tracking Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

87. Specifically, Defendant assisted Facebook in intercepting Plaintiff's and Class Members' electronic communications through the Facebook Tracking Pixel, which tracked,

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

stored and unlawfully disclosed Plaintiff's and Class Members' private and confidential information to third parties, such as Facebook.

88. Defendant assisted in the interception of communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding private and confidential information, including their Facebook ID and treatment information. This confidential information was then monetized for targeted advertising purposes.

89. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

90. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

91. Defendant intentionally intercepted or intentionally assisted in the interception of the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

92. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual,

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

> that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[59]

93. Plaintiff's information that Defendant assisted Facebook in intercepting qualifies as IIHI, and Defendant violated Plaintiff's and Class Members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Facebook Tracking Pixel to track and utilize Plaintiff's and Class Members' private and confidential information for financial gain.

94. Defendant was not acting under the color of law to intercept Plaintiff's and Class Members' wire or electronic communications.

95. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy through the Facebook Tracking Pixel. Plaintiff and Class Members had a reasonable expectation that Defendant would not intercept or assist in the interception of their private and confidential information without their knowledge or consent.

96. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq.*

97. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of the greater of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, *et seq.* under 18 U.S.C. § 2520.

SECOND CAUSE OF ACTION
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631
(On behalf of Plaintiff and the California Subclass)

98. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

[59] 42 U.S.C. § 1320d-6.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

99. CIPA is codified at California Penal Code sections 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . ." Cal. Penal Code § 630.

100. A person violates California Penal Code§ 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

101. Further, a person violates section 631(a) if s/he "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned" in the preceding paragraph. *Id.*

102. To avoid liability under section 631(a), a defendant must show it had the consent of <u>all</u> parties to a communication.

103. At all relevant times, Defendant aided, agreed with, and conspired with Facebook to track and intercept Plaintiff's and Class Members' internet communications while accessing the Website. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

104. Defendant, when aiding and assisting Facebook's wiretapping and eavesdropping, intended to help Facebook learn some meaning of the content in the URLs and the content the visitor requested.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

105. The following items constitute "machine[s], instrument[s], or contrivance[s]" under CIPA, and even if they do not, the Facebook Tracking Pixel falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Facebook used to track Plaintiff and Class Members' communications while they were navigating the Website;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate the Website;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Website; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile device to visit the Website.

106. The information that Defendant transmitted using the Facebook Tracking Pixel, such as information concerning consultations for surgical weight loss procedures, constituted sensitive and confidential PHI and PII.

107. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its patients' sensitive and confidential online communications through the Website without their consent.

108. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 dollars per violation or three times the amount

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

of actual damages. Additionally, California Penal Code section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

109. Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

THIRD CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56.10
(On behalf of Plaintiff and the California Subclass)

110. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

111. Under CMIA, California Civil Code section 56.10, providers of health care are prohibited from disclosing medical information relating to their patients without a patient's authorization. "Medical information" is defined by CMIA as:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. "Individually Identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual . . . .

Cal. Civ. Code § 56.05(j).

112. Plaintiff and members of the California Subclass are patients under the definition in CMIA because Plaintiff and Subclass members received "health care services from a provider of health care" and the information Defendant shared to Facebook was "medical information pertain[ing]" to Plaintiff and Subclass members. Cal. Civ. Code § 56.05(m).

113. Defendant is a "provider of health care", as defined in California Civil Code section 56.05(p), because Defendant offers body contouring, laser liposuction, excess skin removal, and other weight loss medical services. Defendant is also considered a "provider of health care" under California Civil Code section 56.06, subdivisions (a) and (b), because

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

Defendant's Website maintains medical information and offers software to consumers that is designed to maintain medical information for the purposes of allowing its users to manage their information or make the information available to a health care provider, of for the diagnoses, treatment, or management of a medical condition.

114. Therefore, as a provider of health care, Defendant is subject to the requirements of CMIA and had an ongoing obligation to comply with CMIA's requirements regarding the maintenance of its user's medical information.

115. As set forth hereinabove, a Facebook ID is an identifier sufficient to allow identification of an individual. Along with patients' Facebook ID, Defendant disclosed to Facebook several pieces of information regarding its patients' use of Defendant's Website, which, on information and belief, included, but was not limited to: treatment patients were seeking such as scheduling surgical weight loss consultations searched for by prospective patients.

116. This patient information was derived from a provider of health care regarding patients' medical treatment and physical condition. Accordingly, it constitutes medical information pursuant to CMIA.

117. As demonstrated hereinabove, Defendant failed to obtain its patients' valid authorization for the disclosure of medical information.

118. Pursuant to CMIA section 56.11, a valid authorization for disclosure of medical information must: (1) be "[c]learly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or her representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. Accordingly, information set forth in Defendant's Website Privacy Policy does not qualify as a valid authorization.

119. Based on the above, Defendant violated CMIA by disclosing its patients' medical information with Facebook along with the patients' Facebook IDs.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

120. Under CMIA, a patient may recover compensatory damages, punitive damages not to exceed $3,000 dollars and attorneys' fees not to exceed $1,000, and the costs of litigation for any violating disclosure of medical information. Cal. Civ. Code §56.35. Alternatively, a patient may recover nominal damages of $1,000 for any negligent release of medical information. Cal. Civ. Code §56.36.

121. Pursuant to California Penal Code section 637.2, Plaintiffs and Class members have been injured by the violations of California Penal Code section 635, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that this Court enter an Order:

a) Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiff as representative of the Classes, and appointing her counsel as class counsel;

b) Declaring that Defendant's conduct, as set out above, violates the ECPA, CIPA, and CMIA;

c) Awarding statutory damages for each violation of the ECPA, CIPA, and CMIA;

d) Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including an Order requiring Defendant to comply with ECPA, CIPA, and CMIA;

e) Awarding Plaintiff and the Classes their reasonable litigation expenses and attorneys' fees;

f) Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable; and

g) Awarding such other and further relief as equity and justice may require.

CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, Washington 98027
Tel: (425) 837-4717 • Fax: (425) 837-5396

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully Submitted,

T.S., individually and on behalf of all others similarly situated,

Dated: November 25, 2024

By: */s/ Wright A. Noel*

One of Plaintiff's Attorneys

Wright A. Noel
wright@carsonnoel.com
CARSON NOEL PLLC
20 Sixth Avenue NE
Issaquah, WA 98027
Tel: 425.837.4717
Fax: 425.837.5396

Sarah N. Westcot*
swestcot@bursor.com
Stephen A. Beck*
sbeck@bursor.com
BURSOR & FISHER, P.A.
701 Brickell Avenue, Suite 2100
Miami, Florida 33131
Tel: 305.330.5512
Fax: 305.679.9006

**Pro hac vice* admission to be sought.

Attorneys for Plaintiff and the Putative Class